Journal of Number Theory **68**, 29–35 (1998)
Article No. NT972197

Carlitz Modules and Galois Module Structure II

Akira Aiba

Department of Mathematics, Ibaraki University, Mito, Ibaraki 310, Japan

Communicated by D. Goss

Received May 20, 1996

Let $L \supset F$ be cyclotomic function fields of Carlitz. We show that if L/F is Carlitz–Kummer, the integer ring O_L is free over the associated order as in the classical cyclotomic Kummer extension. However, contrary to the characteristic

1. INTRODUCTION

Let L/F be a Galois extension of algebraic number fields with Galois group $\Gamma = Gal(L/F)$, then the ring of integers O_L in L is a module over the associated order

$$A(L/F) = \{\lambda \in F[\Gamma]; \lambda O_L \subset O_L\}$$

of the extension L/F. In several cases, $A(L/F)$-module structure theorems for O_L are obtained. For example, when L is an absolutely abelian extension of $F = \mathbf{Q}$, see [7, 8]. For relative cyclotomic extensions over $\mathbf{Q}$, the following result is classical:

THEOREM 1 ([3] p. 8, Theorem 4.1). *Let m and m' be positive integers with $m \mid m' \mid m^2$, and let ζ_k denote a primitive kth root of unity. Set $F = \mathbf{Q}(\zeta_m)$ and $L = \mathbf{Q}(\zeta_{m'})$. Then*:

$$A(L/F) = \sum_{\chi \in \hat{\Gamma}} O_F e_\chi. \tag{1}$$

Here $\hat{\Gamma}$ denotes the character group of Γ and

$$e_\chi = \frac{1}{\#\Gamma} \sum_{\gamma \in \Gamma} \chi(\gamma^{-1})\, \gamma \in F[\Gamma],$$

the idempotent for $\chi \in \hat{\Gamma}$.

0022-314X/98 $25.00

(2) *O_L is a free rank one $A(L/F)$-module on*

$$\frac{1-\zeta_{m'}^{m'/m}}{1-\zeta_{m'}}.$$

Recently Chan and Lim proved without the condition $m' \mid m^2$ that:

THEOREM 2 ([4.2]). *Let m and m' be positive integers with $m \mid m'$. Set $F = \mathbf{Q}(\zeta_m)$ and $L = \mathbf{Q}(\zeta_{m'})$. Then*:

(1) *A set of generators of $A(L/F)$ as $O[\Gamma]$-module is calculated explicitly.*

(2) *O_L is a rank one free $A(L/F)$-module and a free basis can be constructed explicitly.*

On the other hand we can also consider associated order module structure problems of some other fields with "integer rings". We investigate a positive characteristic analogue of these theorems, using the Carlitz module.

In order to describe our results precisely, we now introduce some notations. Throughout this paper we fix an integer q, which is a power of a prime number p. Let $k = \mathbf{F}_q$ be the field of q elements. Let $K = k(T)$ and $O = O_K = k[T]$, where T is an indeterminate. For a finite extension F of K, we put O_F the integral closure of O in F.

We define some notions about the Carlitz module. For more details, see [5, 6].

DEFINITION. For $M \in O$ we define a polynomial $[M](X) \in O[X]$ as follows.

(1) $[1] = X$

(2) $[T] = X^q + TX$

(3) $[T^n] = [T] \circ [T^{n-1}]$ for $n \geqslant 2$.

(4) If $M(T) = \sum_i a_i T^i$, $a_i \in k$ then $[M] = \sum_i a_i [T^i]$

We put $\Lambda_M = \{x \in K^c; [M](x) = 0\}$, where K^c is algebraic closure of K. It is known that Λ_M is an O-module under the action $u \cdot f = [f](u)$ for $u \in \Lambda_M$ and $f \in O$. Under this action Λ_M becomes a rank one free O/MO-module. We let λ_M be a generator. If $M \mid M'$ are polynomials in O, we have an isomorphism $(1+M)/(1+M') \ni 1 + aM \bmod 1 + M' \mapsto \sigma_{1+aM} \in Gal(K(\Lambda_{M'})/K(\Lambda_M))$, where $\sigma_{1+aM}(\lambda_{M'}) = \lambda_{M'} + [a](\lambda_{M'/M})$.

THEOREM 3. *We put* $M=\prod_{i=1}^{s} P_i^{e_i}$ *and* $M'=\prod_{i=1}^{s} P_i^{f_i}$ $(1\leqslant e_i\leqslant f_i\leqslant 2e_i)$, *where* P_i *is an irreducible polynomial of degree* $d_i\geqslant 1$ *in* O. *Set* $F=K(\Lambda_M)$ *and* $L=K(\Lambda_{M'})$. *Then*:

(1) $A(L/F)=\otimes_i \sum_{j=0}^{q^{d_i(f_i-e_i)}-1} O_F\tau_{i,j}$, *where*

$$\tau_{i,j}=\frac{1}{P_i^{f_i-e_i}}\sum_{N\in O/P_i^{f_i-e_i}}([N](\lambda_{P_i^{f_i-e_i}}))^j\,\sigma_{1+NP_i^{e_i}}$$
$$\in F[Gal(K(\Lambda_{P_i^{f_i}})/K(\Lambda_{P_i^{e_i}}))],$$

for $1\leqslant i\leqslant s$ *and* $0\leqslant j\leqslant q^{d_i(f_i-e_i)}-1$.

(*We identify* $Gal(K(\Lambda_{P_i^{f_i}})/K(\Lambda_{P_i^{e_i}}))$ *with* $Gal(K(\Lambda_{M'})/K(\Lambda_{M'/P_i^{f_i-e_i}}))$.)

(2) O_L *is a free rank one* $A(L/F)$*-module on*

$$\prod_i \lambda_{P_i^{f_i}}^{q^{d_i(f_i-e_i)}-1}.$$

Contrary to Theorem 2, we show that O_L is not free, unless L/F is a Carlitz–Kummer extension (For the definition, see [9]).

THEOREM 4. *We put* $M=\prod P_i^{e_i}$ *and* $M'=\prod P_i^{f_i}$ $(1\leqslant e_i\leqslant f_i$ *for all* i *and* $2e_j<f_j$ *for some* j*). Set* $F=K(\Lambda_M)$ *and* $L=K(\Lambda_{M'})$. *Then* O_L *is not a free* $A(L/F)$*-module.*

2. PROOF OF THEOREM 4

The theorem will be proved in a chain of lemmas which are shown in [1].

LEMMA 1. *Let* E', E *be extensions of* K *such that* E' *over* E *is Galois. Let* $G=Gal(E'/E)$ *be the Galois group and* $A=A(E'/E)$. *Suppose that* $O_{E'}$ *is a free* A*-module* (*necessarily of rank one*). *Then* $A\alpha=O_{E'}$ *if and only if* $\det(\alpha^{\sigma\tau})_{\sigma,\tau\in G}$ *divides* $\det(\beta^{\sigma\tau})_{\sigma,\tau\in G}$ *for all* β *in* $O_{E'}$. (*We will call this* α *minimal and* $\det(\alpha^{\sigma\tau})^2$ *minimal discriminant.*)

LEMMA 2. *Let* p *be a prime number. Let* $G=G_0\times G_1$ *be a finite abelian group, where* G_0 *is the* p*-Sylow subgroup of* G. *Let* f *be a function on* G *with values in some field* E *of characteristic* p. *Then*

$$\det(f(\sigma\tau^{-1}))_{\sigma,\tau\in G}=\prod_{\chi\in\hat{G}_1}\left(\sum_{\tau\in G_0}\left(\sum_{\sigma\in G_1}\chi(\sigma)\right)f(\sigma\tau)\right)^{\#G_0},$$

where $\wedge$ *denotes the group of characters and* $\#$ *the cardinal number.*

LEMMA 3. *Let* $\alpha_1, ..., \alpha_t$ *be arbitrary numbers. Let*

$$\sigma_n = \alpha_1^n + \alpha_2^n + \cdots + \alpha_t^n.$$

We set $f(X) = \prod_j (1 - \alpha_j X)$ *and* $g(X) = \sum_{n=1}^{\infty} \sigma_n X^n$. *Then*

$$g(X) = -Xf'(X)/f(X)$$

LEMMA 4. *Suppose that* $P \in O$ *be a polynomial of degree d. Then* $[P](X) = \sum_{j=0}^{d} \left[\begin{smallmatrix} P \\ j \end{smallmatrix}\right] X^{q^j}$, *where each* $\left[\begin{smallmatrix} P \\ j \end{smallmatrix}\right]$ *is a polynomial in O of degree* $(d-j)\,q^j$. *Especially* $\left[\begin{smallmatrix} P \\ 0 \end{smallmatrix}\right] = P$ *and* $\left[\begin{smallmatrix} P \\ d \end{smallmatrix}\right]$ *is the leading coefficient of P.*
Furthermore, if P is irreducible, then $[P](X) \equiv X^{q^d} \bmod P$.

Substituting

$$G = G_0 = Gal(K(\Lambda_{M'})/K(\Lambda_M))$$

in Lemma 2, we get

$$\det(\alpha^{\sigma\tau^{-1}}) = (\mathrm{Tr}_{K(\Lambda_{M'})/K(\Lambda_M)}\alpha)^{q^m},$$

where m is the degree of M'/M.

Applying Lemma 3 to

$$f(X) = X^{q^m}([M'/M](X^{-1}) - \lambda_M)$$

$$= \sum_{j=0}^{m} \begin{bmatrix} M'/M \\ j \end{bmatrix} X^{q^m - q^j} - \lambda_M X^{q^m},$$

we deduce that (c.f. [1] Lemma 5)

$$\mathrm{Tr}_{K(\Lambda_{M'})/K(\Lambda_M)} \lambda_{M'}^i = \begin{cases} 0 & i < q^m - 1 \\ M'/M & i = q^m - 1. \end{cases}$$

Therefore $\lambda_{M'}^{q^m-1}$ is minimal, for example. We write $r_i = f_i - e_i$. We may assume that $2e_1 < f_1$ and set $P = P_1$, $e = e_1$, $f = f_1$ and $r = r_1$, for simplicity. If we put

$$\tau = \sum_{\alpha \in \mathbf{F}_q} \alpha^{q-2} \sigma_{1 + \alpha P^{r-1} P_2^{e_2} \cdots P_s^{e_s}},$$

then

$$\begin{aligned}\tau(\lambda_{M'}^{q^m-1}) &= \sum_{\alpha} \alpha^{q-2}(\lambda_{M'} + \alpha\lambda_{P^{e+1}P_2^{r_2}\cdots P_s^{r_s}})^{q^m-1} \\ &= \sum_{\alpha} \alpha^{q-2} \sum_{i} \binom{q^m-1}{1} \lambda_{M'}^{q^m-1-i}(\alpha\lambda_{P^{e+1}P_2^{r_2}\cdots P_s^{r_s}})^i \\ &= \sum_{i} \binom{q^m-1}{i} \lambda_{M'}^{q^m-1-i} \lambda_{P^{e+1}P_2^{r_2}\cdots P_s^{r_s}}^{i} \sum_{\alpha} \alpha^{q-2+i} \\ &= \sum_{j=0}^{((q^m-1)/(q-1))-1} \binom{q^m-1}{(q-1)\,j+1} \lambda_{M'}^{q^m-2-(q-1)\,j} \lambda_{P^{e+1}P_2^{r_2}\cdots P_s^{r_s}}^{(q-1)\,j+1}.\end{aligned}$$

Here

$$\begin{aligned}&\lambda_{M'}^{q^m-2-(q-1)\,j} \lambda_{P^{e+1}P_2^{r_2}\cdots P_s^{r_s}}^{(q-1)\,j+1} \\ &\quad \equiv \lambda_{M'}^{q^m-2-(q-1)\,j+q^{d(r-1)+\sum d_i e_i}((q-1)\,j+1)} \qquad \bmod \lambda_M\end{aligned}$$

and the exponent of $\lambda_{M'}$ is

$$\begin{aligned}&q^m-2-(q-1)\,j+q^{d(r-1)+d_2e_2+\cdots d_se_s}((q-1)\,j+1) \\ &\quad = q^m+(q^{d(r-1)+d_2e_2+\cdots+d_se_s}-1)(q-1)\,j \\ &\qquad +(q^{d(r-1)+d_2e_2+\cdots+d_se_s}-2) \geqslant q^m.\end{aligned}$$

Since $\lambda_{M'}^{q^m} \in \lambda_M O_L$, this implies that $(\tau/\lambda_M)(\lambda_{M'}^{q^m-1}) \in O_L$. By Lemma 1, if O_L is $A(L/F)$-free, τ/λ_M must be contained in $A(L/F)$. But

$$\begin{aligned}\frac{\tau}{\lambda_M}(\lambda_{M'}) &= \frac{1}{\lambda_M} \sum_{\alpha} \alpha^{q-2}(\lambda_M + \alpha\lambda_{P^{e+1}P_2^{r_2}\cdots P_s^{r_s}}) \\ &= \frac{\lambda_{P^{e+1}P_2^{r_2}\cdots P_s^{r_s}}}{\lambda_M} \notin O_L.\end{aligned}$$

This is a contradiction.

3. PROOF OF THEOREM 3

We start by proving the prime power case of Theorem 3, that is $F = K(\Lambda_{P^e})$ and $L = K(\Lambda_{P^f})$, where P is an irreducible polynomial of degree d in O_K. We set $r = f - e \leqslant e$. Applying the polynomial $f(X) = X^{q^r}[P^r](X^{-1})$ to Lemma 3, we easily obtain the following lemma.

LEMMA 5. *For any integer* $i \geqq 0$,

$$\sum_{[P^r](\lambda)=0} \lambda^i \equiv 0 \qquad \mod P^r.$$

Moreover

$$\sum_{\lambda} \lambda^i = \begin{cases} 0 & i < q^{dr}-1 \\ P^r & i = q^{dr}-1 \end{cases}$$

and $\sum_\lambda \lambda^i \in P^{r+1}O$ *for* $i > q^{dr}-1$.

PROPOSITION. *For* $j \geqslant 0$,

$$\tau_j = \frac{1}{P^r} \sum_{N \in O/P^r} ([N](\lambda_{P^r}))^j \sigma_{1+NP^e} \in A(L/F).$$

Proof. By the definition of τ_j,

$$\begin{aligned} \tau_j(\lambda_{P^f}^k) &= \frac{1}{P^r} \sum_{N \in O/P^r} ([N](\lambda_{P^r}))^j (\lambda_{P^f} + [N](\lambda_{P^r}))^k \\ &= \frac{1}{P^r} \sum_{N \in O/P^r} \sum_{l=0}^{k} \binom{k}{l} \lambda_{P^f}^{k-l} ([N](\lambda_{P^r}))^{l+j} \\ &= \sum_{l=0}^{k} \binom{k}{l} \left(\frac{1}{P^r} \sum_{N \in O/P^r} ([N](\lambda_{P^r}))^{l+j} \right) \lambda_{P^f}^{k-l}. \end{aligned}$$

Since $(1/P^r) \sum_{N \in O/P^r} ([N](\lambda_{P^r}))^{l+j} \in O$ from Lemma 5, $\tau_j(\lambda_{P^f}^k) \in O$ for all integers $k \geqslant 0$. This completes the proof.

In order to prove the prime power case, it suffices to show that $O_L = \sum_j O_F \tau_j \lambda_{P^f}^{q^{dr}-1}$, for then $O_L = \sum_j O_F \tau_j \lambda_{P^f}^{q^{dr}-1} \supset A(L/F)\lambda_{P^f}^{q^{dr}-1}$ and so by the normal basis theorem.

From Lemma 5,

$$\begin{aligned} &\tau_{q^{dr}-j}(\lambda_{P^f}^{q^{dr}-1}) \\ &\quad = \sum_{k=0}^{q^{dr}-1} \binom{q^{dr}-1}{k} \left(\frac{1}{P^r} \sum_{N \in O/P^r} ([N](\lambda_{P^f})^{q^{dr}-j+k}) \lambda_{P^f}^{q^{dr}-1-k} \right) \\ &\quad \equiv \binom{q^{dr}-1}{j-1} \lambda_{P^f}^{q^{dr}-j} \qquad \mod P, \end{aligned}$$

for $1 \leqslant j \leqslant q^{dr}$. Since $\binom{q^{dr}-1}{j-1}$ is coprime to p for these j's ([10] Lemma 3.8), the transformation matrix from $\{\lambda_{P^f}^j\}_{i=0}^{q^{dr}-1}$ to $\{\tau_j(\lambda_{P^f}^{q^{dr}-1})\}_{j=0}^{q^{dr}-1}$ is invertible

with respect to O_F. The prime power case now follows from the above, since $\{\lambda_{P/}^{i}\}$ is O_F-basis of O_L.

For the general case, one can use induction on the number of prime divisors. (c.f. [4] Section 5)

ACKNOWLEDGMENT

The author is grateful to the referee for his very careful reading of the manuscript and for his comments that improved the presentation of the paper.

REFERENCES

[1] A. Aiba, Carlitz modules and Galois module structure, *J. Number Theory* **62** (1997), 213–219.
[2] W. Bley, A Leopoldt-type result for rings of integers of cyclotomic extensions, *Canad. Math. Bull.* **38** (1995), 141–148.
[3] Ph. Cassou-Noguès and M. J. Taylor, "Elliptic Functions and Rings of Integers," Birkhäuser, 1987.
[4] S. P. Chan and C. H. Lim, Relative Galois module structure of rings of integers of cyclotomic fields, *J. Reine Angew. Math.* **434** (1993), 205–220.
[5] R. J. Chapman, Carlitz modules and normal integral bases, *J. London Math. Soc.* **44** (1991), 250–260.
[6] D. R. Hayes, Explicite class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974), 77–91.
[7] H.-W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, *J. Reine Angew. Math.* **201** (1959), 119–149.
[8] G. Lettl, The ring of integers of an abelian number field, *J. Reine Angew. Math.* **404** (1990), 162–170.
[9] F. Schultheis, Carlitz–Kummer function fields, *J. Number Theory* **36** (1990), 133–144.
[10] M. J. Taylor, Formal groups and the Galois module structure of local rings of integers, *J. Reine Angew. Math.* **358** (1985), 97–103.